DOI: 10.37791/2687-0649-2024-19-3-125-143

Алгоритм стеганографической защиты информации в видеофайлах на основе диффузионно-вероятностной модели с шумоподавлением

***М.И. Дли*[1,2], *А.Ю. Пучков*[1*], *Б.В. Окунев*[1], *И.И. Тищенко*[3]**
[1]*Филиал Национального исследовательского университета «МЭИ» в г. Смоленске, Смоленск, Россия*
[2]*Университет «Синергия», Москва, Россия*
[3]*Управление финансов администрации городского округа – город Волжский Волгоградской области, Россия*
[*]*putchkov63@mail.ru*

Аннотация. Представлены результаты исследования, целью которых являлась разработка алгоритма стеганографии для сокрытия текстовых сообщений в видеофайлах. В основе алгоритма лежит применение диффузионно-вероятностной модели с шумоподавлением, которая реализуется глубокой искусственной нейронной сетью. Алгоритм состоит из двух частей – для передающей и принимающей сообщение сторон. На передающей стороне осуществляется синтез рукописных изображений символов (сигнатур) строки скрываемого сообщения, выравнивание их частотности; применение к сигнатурам прямой диффузии, в результате чего генерируется зашумленное изображение, осаждаемое в видеостегоконтейнер. На приемной стороне проводится извлечение сигнатур из видеоконтента, обратная диффузия для получения сигнатур рукописных символов строки, которые распознаются с помощью сверточной нейронной сети. Новизна исследования заключается в оригинальном разработанном алгоритме стеганографической защиты информации в видеофайлах, а также в модифицированном способе осаждения сигнатур на основе метода замены наименее значащих битов. Способ заключается в побитовом внедрении байтов, характеризующих уровень яркости пикселей в сигнатуре, в одни и те же разряды яркости синего цвета в последовательности из восьми кадров видеостегоконтейнера. Такой способ позволил значительно уменьшить видимые изменения, вносимые в видеоконтент при замене не младших, а средних значащих битов в стегоконтейнере. Это, в свою очередь, обеспечивает большую устойчивость к атакам сжатия при передаче информации по стегоканалу. Практическая значимость результатов исследования состоит в разработанном программном обеспечении, с помощью которого было проведено апробирование алгоритма стеганографической защиты информации в видеофайлах, показавшее высокие значения пикового отношения «сигнал – шум» и индекса структурного сходства изображений при встраивании информации в средние разряды байтов, задающих яркость пикселей стегоконтейнера.

Ключевые слова: стеганография в видеофайлах, глубокие нейронные сети, диффузионно-вероятностные модели

Для цитирования: *Дли М.И., Пучков А.Ю., Окунев Б.В., Тищенко И.И.* Алгоритм стеганографической защиты информации в видеофайлах на основе диффузионно-вероятностной модели с шумоподавлением // Прикладная информатика. 2024. Т. 19. № 3. С. 125–143. DOI: 10.37791/2687-0649-2024-19-3-125-143

Algorithm for steganographic information protection in video files based on a diffusion-probabilistic model with noise reduction

***M. Dli*[1,2], *A. Puchkov*[1*], *B. Okunev*[1], *I. Tishchenko*[3]**
[1]*Branch of the National Research University "MPEI" in Smolensk, Smolensk, Russia*
[2]*Synergy University, Moscow, Russia*
[3]*Finance Department of the City District Administration – Volzhsky city, Volgograd region, Russia*
[*]*putchkov63@mail.ru*

Abstract. The results of a study are presented, the purpose of which was to develop a steganography algorithm for hiding text messages in video files. The algorithm is based on the use of a diffusion-probability model with noise reduction, which is implemented by a deep artificial neural network. The algorithm consists of two parts – for the parties sending and receiving the message. On the transmitting side, the following is carried out: synthesis of handwritten images of symbols (signatures) of the line of the hidden message, alignment of their frequency; applying direct diffusion to signatures, resulting in the generation of a noisy image that is deposited into a video stego container. At the receiving end, signatures are extracted from the video content, back diffusion is performed to obtain signatures of handwritten string characters, which are recognized using a convolutional neural network. The novelty of the research lies in the original developed algorithm for steganographic information protection in video files, as well as in a modified method of signature deposition based on the method of replacing the least significant bits. The method consists of bitwise embedding of bytes characterizing the pixel brightness level in the signature into the same blue brightness digits in a sequence of 8 frames of a video stego container. This method made it possible to significantly reduce the visible changes made to the video content when replacing not the least significant bits, but the middle significant bits in the stego container. This, in turn, provides greater resistance to compression attacks when transmitting information over the stegochannel. The practical significance of the research results lies in the developed software, with the help of which the algorithm for steganographic information protection in video files was tested, which showed high values of the peak signal-to-noise ratio and the index of structural similarity of images when embedding information in the middle bits of the bytes that set the brightness of the pixels of the stego container.

Keywords: steganography in video files, deep neural networks, diffusion-probabilistic models

For citation: Dli M., Puchkov A., Okunev B., Tishchenko I. Algorithm for steganographic information protection in video files based on a diffusion-probabilistic model with noise reduction. *Prikladnaya informatika*=Journal of Applied Informatics, 2024, vol.19, no.3, pp.125-143 (in Russian). DOI: 10.37791/2687-0649-2024-19-3-125-143

Введение

Охрана интеллектуальной собственности и конфиденциальных данных (персональных данных, коммерческой тайны и др.) от несанкционированного доступа принадлежит к числу наиболее значимых задач информационной безопасности. Многообразие методов и алгоритмов, предложенных для ее решения, не могут считаться универсальными и действенными инструментами за исключением квантовых систем и каналов связи, которые к настоящему времени ввиду